Claims: Cancel all claims of record and substitute new claims 1 to 18 as follows:

What is claimed is as follows:

1. A computer-related method and software apparatus for the prevention, detection and reclamation related to criminal or unauthorized Identity theft, comprising:

a plurality of data storage devices (DSD);

a memory which is able to replicate a plurality of databases of public or private, legal or illegal origination;

a memory which is able to store a plurality of data points related to or commonly used in financial transactions;

a input screen which a human end user can use to store their data points;

a data store of said information for a plurality of end users, including end users' preference of action when Identity theft occurs as against said end users;

a communication port suitable for transmitting and receiving data and instructions in the form of electrical signals, to and from remote computers of both end users and said plurality of databases and said memories;

a communication port where said end users and said memory controllers and communication port is on or operates via the Internet.

a memory which is able to store a plurality of said indicia;

a memory which is able to persistently scan public and private networks for transmissions of data points which are relevant to said end users;

a memory which is a metadata table to store lists of locations of the said databases;

a memory which monitors all transmitted data to and from said end users to encrypt and decrypt information for the protection of said end users;

a output screen which will notify said end users when Identity theft or the indicia of Identity theft is detected;

a memory controller that persistently compares information contained in said databases to that of end user data points and to the database and memory of known Identity theft related indicia;

a memory controller that persistently provides notification of the statistical or anecdotal indicia of incorrect or illegally appropriated data points;

a memory controller that persistently provide an automated means to update memory with new and changing indicia;

a memory controller that persistently or occasionally notifies end users when new information from said databases is found;

a memory controller that reactively provide a variety of options for automated restoration or correction of incorrect or illegally appropriated data points;

a memory controller that reactively performs said automatic restoration or correction or reversal of unauthorized charges at end users discretion, and;

a memory controller that reactively provide electronic notification to law enforcement in certain situations and at end users discretion;

Whereby new and existing information said databases will be scanned and compared to end user data, and

Whereby end users are protected from unauthorized personal identity data point appropriation as it occurs and further optionally take steps to immediately avoid the loss associated with unauthorized personal identity data point appropriation.

2. A method according to claim one comprising the searching of data related to possible Identity theft gathered through an internet content indexing system, also known as web spidering, comprising the steps of:

a memory which replicates said plurality of data sources means optionally receiving persistent updates over public or private networks so as to create a persistent replica of said data sources so said searching and analysis may be performed in a private and secured location;

a memory which searches for end user data from private and protected instances of said plurality of data sources;

a communications port communicating via public and secure channels on the Internet

persistently monitoring national or international financial clearance networks;

persistently scanning said databases to add, update or delete the location of said databases;

persistently scanning and compares information contained in said databases to that of end users;

updating memory with recordation of found matching or related data points;

persistently monitoring national and international credit card transactions and create database entries when transactions pertaining to end users occur;

Securing and encrypting the DSD containing subscriber data

transmitting of all communication optionally over the public internet using a Secured Socket Layer (SSL) or successor standards for secured, on-line communication;

Whereby new and existing information said databases will be scanned and compared to end user data, and

Whereby end users are protected from unauthorized personal identity data point appropriation as it occurs and further optionally take steps to immediately avoid the loss associated with unauthorized personal identity data point appropriation.

3. A method and process according to claim one and two which culls, analyzes compares, and analyzes said end user data points against statistical or anecdotal indicia of unauthorized personal identity data point appropriation further comprising the steps of:

Communicating via a port communicating via public and secure channels on the Internet or via private internet;

persistently monitoring national or international financial clearance networks;

persistently scanning said databases to add, update or delete the location of said databases;

persistently scanning and compares information contained in said databases to that of current database;

updating memory with recordation of found matching or related data points;

Whereby new and existing information said databases will be scanned and compared to end user data, and

Whereby a plurality of data sources are compared to said end user's data.

4. A method according to claim one, where said plurality of data sources is persistently updated comprising the steps of:

a memory controller that persistently compares end user data and provides notification of the statistical or anecdotal indicia of incorrect or illegally appropriated data points;

storing an image of each database comprising said plurality of data sources;

comparing image of original data sources to said replicated plurality of databases;

persistently monitoring national and international credit card transactions and create database entries when transactions pertaining to end users occur;

a memory controller that persistently provides an automated means to update memory with new and changing indicia;

a memory controller securing and encrypting the DSD containing subscriber data;

a communications port which transmits all communication optionally over the public internet using a Secured Socket Layer (SSL) or successor standards for secured, on-line communication or via the public internet when appropriate,

a memory controller that connects to public or private newsgroups or chat rooms or other venues that are commonly used locations for the trade or sale of illegally obtained data, said memory posing as a buyer, seller or trader of said illegal information, using an assumed and fictitious identity and can perform transactions yielding said illegally obtained data, using same as a source of information to prevent Identity theft, and;

a memory controller that updates a plurality of databases, or data points therein, when changes are detected, and;

An HTML (hypertext markup language) page group representing levels of threat related to said Identity theft and its associated risk graphically as against the end user's risk level using common graphical metaphors.

Whereby new and existing information said databases will be scanned and compared to end user data, and

Whereby data sources are persistently updated to insure timeliness of data which may represent the said indicia of said Identity theft.

5. A method according to claim one further comprising notification to end users when said indicia of said Identity theft occurs, via the public internet or via private networks further comprising the steps of:

a memory for notification of end users is made to end users' wireless, handheld or other portable devices, and;

a memory for notification to end users of said indicia via electronic mail, and;

a memory for notification to end users of said indicia via graphical web pages, and;

a memory for providing an end user options for reversal or repair of said Identity theft.

Whereby new and existing information said databases will be scanned and compared to end user data, and

Whereby end users are notified of apparent Identity theft.

6. A method of claim one, which is a computer software method of prevention, reversal or repair of said by submitting notice to government agencies, private data providers and the maintainers of public record databases when end user's data points are incorrect, misleading or the indicia of Identity theft has met a specified threshold, further comprising the steps of:

submitting automated requests for an end user to be excluded from certain databases, as pre-defined by end users, to the maintainers of said certain databases, and;

informing maintainers of government databases when said indicia of Identity theft occurs, so that information may be removed or altered,

and;

spontaneously or occasionally canceling an authorized transaction related to an occurrence of Identity theft, and;

informing a single or plurality of replicated databases provided by credit bureaus and only credit bureaus

a memory printing appropriate paper forms and reports for submission to maintainers of said data sources, law enforcement agencies, creditors, debtors or security specialists, where said maintainers are unable or unwilling to accept electronic notice.

Whereby end users are notified, pursuant to their profile, of any indicia of Identity theft and

Whereby end users are protected from unauthorized personal identity data point appropriation as it occurs and further optionally take steps to immediately avoid the loss associated with unauthorized personal identity data point appropriation.

7. A method of claim one or where said end users are informed of the said indicia of a said Identity theft, via wireless, handheld, portable devices, electronic mail, or graphical web pages.

Whereby end users are informed of the indicia of Identity theft by a plurality of means, and afforded the opportunity to commence the actions detailed herein to stop said Identity theft, and

Whereby end users are notified regarding unauthorized Identity theft as it occurs and prompted to take optional steps to immediately avoid the loss associated with unauthorized personal identity data point appropriation.

8. A method of claim one, which is a computer software means of prevention, reversal or repair of said by submitting notice to law enforcement and government agencies, to expedite investigation and enforcement and reversal of said Identity theft.

Whereby said indicia of Identity theft is automatically or rapidly provided to law enforcement and government agencies

Whereby end users are protected from unauthorized personal identity data point appropriation as it occurs and prompted with the option of

reporting said Identity theft to law enforcement and government agencies.

9. A method of claim one, where the present invention is offered via private networks using replicated source databases said replication performed over a secured internet channel, so said analysis can be performed in a secure location, thereby effecting said analysis without any risk associated with broadcasting end user data points over a public network, such as the internet.

Whereby source databases are replicated over a secure channel on a private network, to allow searching for the indicia of Identity theft without public disclosure of any end user data.

Whereby end users are protected from unauthorized personal identity data point appropriation as it occurs and further optionally take steps to immediately avoid the loss associated with unauthorized personal identity data point appropriation.

10. A method for protecting against identity theft, comprising:

obtaining initial personal and credit information from a end-user;

obtaining a first report of personal and credit information about the end-user from at least one credit agency or information source;

obtaining, after a predetermined amount of time, a second report of personal and information about the end-user from the credit agency or information source;

comparing the second report of personal and credit information obtained from the credit agency or information source with the first personal and credit information obtained from the credit agency or information source;

identifying discrepancies between the second report of personal and credit information obtained from the credit agency or information source and the first report of personal and credit information obtained from the credit agency or information source;

verifying discrepancies between the second report of personal and credit information obtained from the credit agency or information source and the first report of personal and credit information obtained from the credit agency or information source with the end-user;

correcting discrepancies not verified by the end-user between the second report of personal and credit information obtained from the credit agency or information source with the first report of personal and credit information

obtained from the credit agency or information source; and

repeating steps c through g.

11. The method of claim 10 further comprising the steps comparing the initial personal and credit information obtained from the end-user with the first report of personal and credit information obtained from the credit agency or information source;

identifying discrepancies between the initial personal and credit information obtained from the end-user and the first report of personal and credit information obtained from the credit agency or information source; and

correcting discrepancies between the first report of personal and credit information obtained from the credit agency or information source and the initial personal and credit information obtained from the end-user.

12. The method of claim 10 wherein the predetermined amount of time is selected from the group consisting of a day, a week, a month, a quarter, six months and a year.

13. The method of claim 10 wherein the predetermined amount of time is a week.

14. The method of claim 10 wherein the predetermined amount of time is a month.

15. The method of claim 10 wherein the predetermined amount of time is less than one minute.

16. The method of claim 10 wherein the at least one credit agency or information source is one or more agencies selected from the group consisting of Equifax, Experian and TransUnion, or of their successor interests.

17. The method of claim 10 where information about said discrepancies is delivered using the internet or other communication ports, such as those controlling cell phones and wireless devices.

18. The method of claim 10 where the internet is the primary mode of communication.

REMARKS - General

By the above amendment, Applicant has amended the title to emphasize the novelty of the invention.

Also applicant has rewritten all claims so as to define the invention more particularly and distinctly so as to overcome the technical rejections and define the invention patentably over the prior art.

The Rejections to the Specification And the Claims Rejection Under § 112. The Specification and all claims were rejected pursuant to § 112 because it was said to have no explanation of how the elements would work.

Applicant requests reconsideration and withdrawal of this objection since by this amendment the claims are described more particularly and distinctly.

The Rejections Under § 102(E) As Being Anticipated By Freishtat *Et Al.* Is Overcome

The last O.A. rejected claims 1-9 as being anticipated by Freishtat et al., US # 6,317,783 B1. Claims 1-9 are rewritten to describe the present invention with more particularity.

Freishtat discloses an internet related method for aggregation of personal information for direct marketing and purposes of marketing and end user convenience. It does not identify or respond to crimes of any type. *Freishtat* is concerned with personal information only to the extent that information would become a portal for an end user.

The present invention yields the unobvious result of stopping identity related crimes. Such a result, intended or unintended, is nowhere found in *Freishtat.*

The Objections Related to Punctuation is overcome

All claims have been rewritten to be correctly punctuated.

The Conclusion that Prior Art Made Of Record and Not Relied Upon is Considered Pertinent To Applicant's Disclosure (With Regard To US# 6,253,203 B1) Is Overcome

O'Flaherty teaches of systems and methods of data warehousing and analysis, and in particular to a system and method for enforcing privacy constraints on a database management system. This is not the object of the present invention. Further, one reading of *O'Flaherty* suggests what is disclosed is a tool for providing some measure of consumer privacy, while providing data necessary for certain marketing practices.

The present invention does not contemplate marketing or a particular means or mechanism of storing personal information. The present invention yields the unobvious result of stopping identity related crimes. Such a result, intended or unintended, is nowhere found in *O'Flaherty.*